UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,364	01/23/2004	Roger Maitland	Q102939	4471

23373 7590 05/23/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/762,364	**Applicant(s)** MAITLAND ET AL.	
	Examiner ELLEN TRAN	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _11 January 2008_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-79_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-79_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to: amendment filed on 11 January 2008 with an original application filed on 30 September 2004 and acknowledgement of a provisional application 60/545,928 filed 20 February 2004.

2. Claims 1-79, are currently pending. Claims 1, 12, 21, 35, 49-51, 55, 64, and 73-76, are independent claims. Claims 1, 3-7, 9, 10, 12, 14-25, 27-30, 33-39, 41-45, 47-52, 54, 57, 59, 61, 64, 66-68, 70, 71, 73-76 are amended. Claims 77-79 are new. Amendment to the claims is accepted.

Response to Arguments

3. The Objections to the claims have been removed due to amendment.

4. Applicant's arguments with respect to the prior art rejection have been fully considered but they are not persuasive.

I) In response to applicant's argument on page 27 *"The examiner has not identified look-up tables in Kim"*. The Examiner disagrees with argument the look-up tables were shown in Luyster. It is the combination of references that teaches the invention Kim is directed to a Kasumi encryption system, Luyster is directed to a block cipher method utilizing s-box and bit-permute rounds. Note s-box are equivalent to look-up tables see Luyster col. 4, lines 59-60 "These so-called s-boxes are substitution boxes or, simply look-up tables". In addition as understood by Kasumi Specification the functions S7 and S9 are s-box or look-up tables, see section 4.4 and 4.5. on pages 11-12. Therefore the Kim reference is utilizing lookup tables when it applies the 7-bit and 9-bit FI function as explained on page 9.

II) In response to applicant's argument on page 27 *"nor has the examiner identified which of the bits of the input are considered to be the claimed first set of bits and which are considered to be the claimed second set of bits"*. The Examiner disagrees with argument the Kim reference on page 9 defines that the 32 bit input are separated into 16 upper and lower bit data. The upper 16 bit data is also separated into 9-bit and 7-bit data. Note the separation of the 32 input bit is interpreted to be equivalent to the "set of bits".

III) In response to applicant's argument on page 27, *"But it is in any event clear that in the operation of Kim there is no point at which the first set is used form some process and second set is used to select from the result of processing the first set"*. The Examiner disagrees with argument, the limitation of: "the first set is used for some process and second set is used to select from the result of processing the first set" is not in the claims. In addition as shown by Kim the output of the first 16-bit, S7 and S9 operation is utilized in the second pipeline that uses the 16-bit input data separated from the 32-bit input.

IV) In response to applicant's argument on page 28, *"But this Exclusive OR operation is not the selection of one of the output data bits as required by claim 1"*. The Examiner disagrees with argument and again notes the references should be reviewed in combination. Kim teaches a first set and second set of bits. Kim also teaches that the output of the first set is utilized with the second set for the output. Note the look-up tables are taught in Luyster, col. 17, lines 30-37 which teaches "the nonlinear function is an s-box and the system generally includes a s-box linear combination functions which uses a round operator generally from a second algebraic group executable on the computing unit which combines a one-to-one round segment with the output of an s-box lookup of a value which depends on a preselected number of bits from a preselected location in a different one-to-one round segment".

V) In response to applicant's argument on page 28, *"The '319 patent teaches a block cipher method, but does not make up for this deficiency in Kim. Thus, even if the teachings of he references were combined in some obvious manner, there would be no selection of one of the outputs from the processing of the first set of input bits, as is required in independent claims 1, 12, and 49"*. The Examiner disagrees with argument and notes the combination teaches the first set of outputs is used with the second set. Note the Kim reference utilizes the Kasumi algorithm in which the inputs are divided into 32 bits and then 7-bit and 9-bit, the result of these inputs is utilized in the second pipeline section.

VI) In response to applicant's argument on page 28 *"With respect to claim 21, note that the claim requires that there be plural inputs each of plural bits, and a selection of a subset of the input bits. This requires multiple subsets selected from multiple parallel inputs. The examiner cites to page 9 of Kim, buts has not identified what is considered to be the claims plurality of inputs. There is one 32-bit inputs in Fig. 4 of Kim. There is a selection of a subset of the input, but this selection os a subset of the input is not performed for multiple inputs in parallel. That would require replicating Fig. 4 of Kim to have multiple pipeline sequences, but this is not suggested in Kim"*. The Examiner disagrees with argument and notes as explained in Kim the inputs are divided in 16 bits, the first group of 16 bits is utilized in the first pipeline. The first pipeline uses 9-bit and 7-bit in parallel, note 9 and 7 are a plurality. In addition 7 is less than nine. In addition as explained above the Kim reference implements the Kasumi algorithm which utilizes s-boxes for the 9-bit and 7-bit input section these outputs are fed into the second pipeline.

VII) In response to applicant's argument on page 29, *"As to claim 51, the examiner simply reads the claim language broadly refers to page 9 of Kim, but the subject matter of claim 51 is not found there. Claim 51 requires that plural inputs each made up of plural bits. Bit re-ordering is performed on the plural-bit inputs to obtain M parallel outputs. The examiner has not identified where the plural bit inputs are, or where the bit re-ordering takes place. The examiner has further not identified where the ith set of those outputs is, or how it defines a respective subset of the input bits. This is simply not taught in Kim, or in any of the secondary art"*. The Examiner disagrees with arguments for multiple reasons. The references as a whole should be reviewed Kim teaches the Kasumi algorithm, the Kin and Kout bits as well as the bit rotation on shown in FIG. 2, also see page 6, lines 1-18.

VIII) In response to applicant's argument on page 29, *"As to claim 55, the claim defines a ciphering method in which there are a plurality of ciphering algorithm inputs, a plurality of first inputs each associated with one of the ciphering algorithm inputs, and each first input is used to address a lookup table ... Claim 55 requires that there be plural lookup tables each addressed by a respective first input, with all of this done in parallel"*. The Examiner disagrees with argument as stated above. Kim teaches the Kasumi algorithm the 16-bit input is separated into 7-bit and 9-bit utilizing the S7 and S9 Kasumi algorithm, s-box or lookup tables. This is taught in Kim, in addition the Luyster references teaches the lookup tables.

IX) In response to applicant's argument beginning on page 29, *"As to claims 74-76, these claims require that a plurality of inputs each be used to address respective lookup tables to provide respective outputs. Bt it is noted that in Fig. 4 of Kim et al, the output of the first stage 210 is only obtained by Exclusive ORing the processed result of the ... Even if look-up tables* *were to be used in the Kim et al system, the examiner has not explained".* The Examiner disagrees with applicant, as explained above the Kim reference teaches the Kasumi algorithm the lookup tables are used with the S7 and S9 operations.

Note this action is a Non-Final even though the same references were used. The Action has been updated to include a 101 Rejection to appropriate claims. In addition more details are included in the rejection.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 49, 50, 73, 76, and 79, are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 49, 50, 73 and 76 as well as dependent claims 79 are directed to "An article of manufacture comprising: a computer readable medium program code means". Therefore because a computer readable program code means is non-statutory subject matter, Claims 49, 50, 73, 76, and 79 are rejected. Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

> matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 74-79,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter '784) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter '319).

As to independent claim 74, A method comprising the step of, responsive to a plurality of inputs, each input being defined by at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs" is taught in '784 on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;the following is not explicitly taught in '784:

"looking-up a look-up table having a plurality of elements using the at least one bit that define the input to obtain an output" however '319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see '319 (col. 4, line 54 through col. 5, line 3) " A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

As to independent claim 75, this claim is directed to the apparatus executing the method of claim 74; therefore it is rejected along similar rationale.

As to independent claim 76, this claim is directed to an article of manufacture executing the method of claim 74; therefore it is rejected along similar rationale.

9. **Claims 1, 2, 5, 6, 11-13, 16, 21-28, 30, 31, 33-42, 44, 45, 47-73, and 77-79,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter '784) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter '319) in further view of 3GPP TS 35.202 v3.1.1 Release 1999 (hereinafter 3GPP).

As to independent claim 1, "A method comprising responsive to a plurality of inputs, each input being defined by a first set of bits and a second set of at least one bit, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs:" is taught in '784 on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

the following is not explicitly taught in ‘784:

“for each of a plurality of look-up tables each having a plurality of elements, looking-up one of the plurality of elements of the look-up table using the first set of bits that define the input to obtain an output, the output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see ‘319 (col. 4, line 54 through col. 5, line 3) “ A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers”.

the following is not explicitly taught in ‘784 and ‘319:

“and selecting a corresponding output from the set of corresponding outputs using the second set of a least one bit that defines the input” however ‘3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 and ‘319 to utilize the KASUMI documentation in order to clarify the invention taught in '784. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in ‘784, the invention is directed to an improvement of the convention implementation apply the KASUMI algorithm in the 3GPP system (see ‘784 page 2, lines 3 et seq.) “However, since the convention implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic cause the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency”.

As to dependent claim 2, "wherein the plurality of elements of each look-up table collectively comprise a combined table of elements each having a pre-determined value obtained using an S7 function" is taught in '784 page 11, lines 4-10.

As to dependent claim 5, "wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises one bit and the set of corresponding outputs comprises two corresponding outputs, and wherein for each of the plurality of inputs the selecting comprises: selecting one of the two outputs using the one bit of the at least one bit that defines the input" is taught in '784 page 4, lines 30-35.

As to dependent claim 6, "wherein for each of the plurality of inputs, the second set of at least one bit that defines the input comprises at least two bits, and wherein for each of the plurality of inputs the selecting comprises: successively performing a selection on a remaining number of corresponding outputs of the set of corresponding outputs for each bit of the at least two bits, the number of corresponding outputs remaining being equal to all of the corresponding outputs of the set of corresponding outputs a first time the selection is performed, the selection being replacing the remaining number of corresponding outputs with a selection of half of the remaining number of outputs using a respective bit of the at least two bits, the selection of half of the remaining number of outputs being the number of remaining outputs for the next time the selection is performed" is shown in '784 page 6, lines 8-29.

As to dependent claim 11, "applied in ciphering data in a Kasumi implementation" is taught in '784 page 2, lines 25-33.

As to independent claim 12, this claim is directed to the apparatus executing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 13 and 16, these claim contain substantially similar subject matter as claims 2, 5, and 6; therefore they are rejected along similar rationale.

As to independent claim 21, "A method comprising: responsive to a plurality of inputs, each input being defined by a first plurality of bits, for each input of the plurality of inputs and in parallel with other inputs of the plurality of inputs" is taught in '784 on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

"selecting a respective subset of bits of the first plurality of bits that define the input, the bits of the respective subset of bits comprising fewer bits than the first plurality of bits of the input" is shown on page 9, lines 13-31, note of the 32 input bits 16 are separated and applied to 9-bit and 7-bit of the FI function defined in the KASUMI encryption;
the following is not explicitly taught in '784:

"and looking-up an element of the plurality of elements of the look-up table using the subset of bits to obtain an output"; however '319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see '319 (col. 4, line 54 through col. 5, line 3) " A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

the following is not explicitly taught in '784 and '319:

"and for each of a plurality of look-up tables each having a plurality of elements" and "and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit" however '3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 and '319 to utilize the KASUMI documentation in order to clarify the invention taught in '784. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in '784, the invention is directed to an improvement of the convention implementation apply the KASUMI algorithm in the 3GPP system (see ‘784 page 2, lines 3 et seq.) “However, since the convention implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic cause the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency”.

As to dependent claim 22, “wherein for each input of the plurality of inputs, the outputs obtained from the plurality of look-up tables each comprise a second plurality of bits, the second plurality of bits comprising fewer bits than the first plurality of bits of the input” is shown in ‘784 page 10, lines 9-15.

As to dependent claim 23, “wherein for each input of the plurality of inputs, the at least one bit comprises a third plurality of bits, the third plurality of bits comprising the same number of bits as the first plurality of bits of the input” is shown in ‘784 page 10, lines 9-15.

As to dependent claim 24, “wherein for at least one look-up table of the plurality of look-up tables, for each input the selecting comprises manipulating at least one of the plurality of bits that define the input using at least one of a bit rotation instruction and a bit shifting instruction” is disclosed in ‘784 page 6, lines 1-29.

As to dependent claim 25, "wherein for each of the at least one look-up table, for each input the manipulating at least one of the first plurality of bits comprises ordering the respective subset of bits of the input as least significant bits" is taught in '784 page 9, lines 7-31.

As to dependent claim 26, "wherein each element of the plurality of elements of each look-up table has a pre-determined value" however '319 teaches loading predetermined values into tables in col. 38, lines 24-36.

As to dependent claim 27, "wherein for each input of the plurality of inputs the first plurality of bits and the third plurality of bits each comprise 9 bits, the pre-determined value of each of the plurality of elements of each of the plurality of look-up tables is obtained from a partial evaluation of an S9 function" is shown in '784 page 9, line 32 through page 10, line 8.

As to dependent claim 28, "wherein for each look-up table of the plurality of look-up tables, the pre-determined value of each of the plurality of elements of the look-up table is a function of a number being definable by a bit sequence of one of 4 and 5 bits" is disclosed in '784 page 13, lines 9-16.

As to dependent claim 30, "wherein for each input of the plurality of inputs, the combining comprises performing a plurality of exclusive-OR operations on the outputs obtained from the plurality of look-up tables for the input" is taught in '784 page 9, lines 9-31.

As to dependent claim 31, "wherein for each input of the plurality of inputs, the combining comprises manipulating the second plurality of bits of at least one output of the outputs obtained from the plurality of look-up tables for the input using one of a bit shifting instruction and a bit rotation instruction" is shown in '784 page 9, lines 9-31.

As to dependent claim 33, "wherein for each input of the plurality of inputs, the combining comprises: for a first output of the outputs obtained from the plurality of look-up tables for the input, manipulating the second plurality of bits of the first output using one of a bit rotation instruction and a bit shifting instruction; and for a second output of the outputs obi;aired from the plurality of look-up tables for the input, performing one of the plurality of exclusive-OR operations on the second output and the first output to obtain a third output having a fourth plurality of bits" is disclosed in '784 page 9, lines 9-31.

As to dependent claim 34, "wherein for each input, the bits of the second plurality of bits of each respective subset of bits of the first plurality of bits of the input have a pre-determined order and are each used for obtaining a respective one of the third plurality of bits, the outputs obtained from the look-up tables collectively comprising at least one group of outputs each having at least two outputs of the outputs obtained from the look-up tables" however '319 teaches lookup tables in col. 15, lines 48-55;

"for each group of outputs of the at least one group of outputs the at least two outputs in the group of outputs having bits used for determining a common subset of bits of the third plurality of bits, the combining comprising: for each group of outputs of the at

least of group of outputs, combining the at least two outputs of the group of outputs using at least one of the plurality of exclusive-OR operations" is shown in '784 page 5, lines 10-36.

As to independent claim 35, this claim is directed to the apparatus executing the method of claim 21; therefore it is rejected along similar rationale.

As to dependent claims 36-42, 44, 45, 47, and 48, these claim contain substantially similar subject matter as claims 22-28, 30, 31, 33, and 34; therefore they are rejected along similar rationale.

As to independent claim 49, this claim is directed to an article of manufacture of the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 50, this claim is directed to an article of manufacture of the method of claim 21; therefore it is rejected along similar rationale.

As to independent claim 51, "A method comprising, responsive to N K_{in}-bit inputs: performing bit reordering on the N K_{in}-bit inputs to produce M parallel sets of outputs wherein N and K_{in} are integers satisfying N, $K_{in} \geq 2$" is taught in '784 on page 6, lines 1-29, Kim teaches the Kasumi algorithm, the Kin and Kout bits as well as the bit rotation on shown in FIG. 2 ;

"an ith set of outputs of the M parallel sets of outputs containing N sets of bits $L_{i,in}$ bits in length with i and $L_{i,in}$ being integers satisfying i=1 to M and $1 \leq L_{i,in} < K_{in}$, the ith set of outputs defining a respective subset of the K_{in} bits of the inputs" is taught in '784 on page 9, lines 8-31, note the first pipeline stores upper 16-bit data of the 32-bit input. The upper 16-bit data is interpreted to be equivalent to Li, in a first set of bits, the lower 16-bit data is interpreted be equivalent to the second set, and simultaneously is interpreted to be equivalent to in parallel;

the following is not explicitly taught in ‘784:

“for each parallel set of outputs, performing a parallel lookup table operation to generate a corresponding parallel set of outputs containing N outputs, each being associated with a respective one of the N K_{in}-bit inputs and each being $L_{i,out}$ bits in length” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see ‘319 (col. 4, line 54 through col. 5, line 3) “ A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers".

the following is not explicitly taught in '784 and '319:

"$L_{i,out}$ being an integer satisfying $L_{i,out} \geq 1$; and for each of the N K_{in}-bit inputs, generating a respective output by performing a bit combining operation on the outputs from the parallel look-up table operations associated with the input" however '3GPP teaches on page 11-12 sections 4.4 and 4.5 that the output from the first bit string are utilized for inputs to the second string (or second set of at least one bit). Note the s-box is interpreted equivalent to the lookup tables.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 and '319 to utilize the KASUMI documentation in order to clarify the invention taught in '784. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in '784, the invention is directed to an improvement of the convention implementation apply the KASUMI algorithm in the 3GPP system (see '784 page 2, lines 3 et seq.) "However, since the convention implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic cause the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency".

As to dependent 52, "wherein for each of the N K_{in}-bit inputs, the generating comprises performing a bit manipulation on the outputs of the parallel look-up table operations associated with the input" is disclosed in '784 page 6, lines 1-29.

As to dependent 53, "wherein the bit combining operations are implemented in parallel" is taught in '784 on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel.

As to dependent claim 54, "wherein for each of the N K_{in}-bit inputs the respective output generated K_{out} bits, K_{out} being an integer satisfying $K_{out} \geq 1$, and wherein in performing the bit permutation/reordering on the N K_{in}-bit inputs, the ith set of outputs defining the respective subset of the K_{in} bits of the inputs is selected such that the respective subset of the K_{in} bits effects only a defined maximum number Pi< K_{out} bits of the respective outputs wherein Pi is an integer" is disclosed in '784 page 6, lines 1-29.

As to independent claim 55, "A method of generating a plurality of outputs according to a ciphering algorithm which for each of the plurality of outputs operates on a respective input using a respective key" is taught in '784 page 6, lines 5-18, note Kim teaches that the key registers store keys that are rotated;

"responsive to a plurality of first inputs each being associated with one of the respective inputs, for each first input and in parallel with other first inputs of the plurality of first inputs:" is taught on page 9, lines 8-31, note simultaneously is interpreted to be equivalent to in parallel;

the following is not explicitly taught in '784:

“generating an output by looking up at least one look-up table using the input, each look-up table having a plurality of elements” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in ‘784 to include a means to utilize look-up tables. One of ordinary skill in the art would have been motivated to perform such a modification in order to save memory see ‘319 (col. 4, line 54 through col. 5, line 3) “ A good example of perhaps the first historically significant symmetric cryptographic system (i.e., when the same key is used in the encipherment and decipherment transformations) is the Data Encryption Standard ("DES"), which is a U.S. Government standard. DES uses small "s-boxes" to provide security. These so-called s-boxes are substitution boxes or, simply, look-up tables. S-boxes provide output which is a nonlinear function of the input, based on a lookup table. Small s-boxes are lookup tables with a small number of possible inputs. Often, small s-boxes have a small number of output bits as well. For example, each s-box of DES has 6-bit inputs or 64 possible inputs and 4-bit outputs or 16 possible output values. They do not require much memory; nor does it take long to load them in microprocessor memory. S-boxes are generally stored in on-chip cache, generally the next quickest form of microprocessor memory after registers”.

the following is not explicitly taught in ‘784 and ‘319:

“the ciphering algorithm comprising a plurality of rounds in which functions are evaluated, the method comprising, for at least one function of the functions of at least one

of the plurality of rounds:" however 3GPP teaches that the Kasumi algorithm is a plurality of functions that are evaluated in the round functions see page 10, section 4.1.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 and '319 to utilize the KASUMI documentation in order to clarify the invention taught in '784. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in '784, the invention is directed to an improvement of the convention implementation apply the KASUMI algorithm in the 3GPP system (see '784 page 2, lines 3 et seq.) "However, since the convention implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic cause the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency".

As to dependent claim 56, "wherein the ciphering algorithm is a Kasumi algorithm" is taught in '784 page 2, lines 25-33.

As to dependent claim 57, "wherein for a function of a certain type of the at least one function the at least one look-up table comprising a plurality of look-up tables and the output from each of the plurality of look-up tables collectively comprising a set of corresponding outputs" however '319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

“each first input of the plurality of first inputs being defined by a first set of bits and a second set of at least one bit, the method comprising for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs:” is taught in ‘784 on page 9, lines 8-31;

“selecting a corresponding output from the set of corresponding outputs using the second set of at least one bit that defines the input” is shown in ‘784 page 6, lines 8-29.

As to dependent claim 58, “wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S7 function” is taught in ‘784 page 11, lines 4-10.

As to dependent claim 59, “wherein, for a function of a certain type of the at least one function the at least one look-up table comprises a plurality of look-up tables and each first input of the plurality of first inputs is defined by a first plurality of bits, the method comprising:” however ‘319 teaches that the s-box or lookup table is used with encryption in col. 17, lines 30-51;

“for each first input of the plurality of first inputs and in parallel with the other first inputs of the plurality of first inputs, and for each of the plurality of look-up tables: selecting a respective subset of bits of the first plurality of bits that define the first input, the bits of the respective subset of bits comprising fewer bits than the first plurality of bits of the first input, the look-up table being looked up using the subset of bits to obtain the output” is shown in ‘784 page 6, lines 8-29;

“and combining the outputs obtained from the plurality of look-up tables to obtain at least one bit” is taught in ‘784 page 2, lines 25-33.

As to dependent claim 60, "wherein the ciphering algorithm is a Kasumi algorithm and the function of a certain type is an S9 function" is taught in '784 page 11, lines 4-10.

As to dependent claim 61, "wherein the at least one round comprises the plurality of rounds and wherein for each round the at least one function comprises six S7 functions and six S9 functions, the method further comprising for each function of the plurality of functions other then the at least one function, and responsive to a plurality of second inputs each being associated with one of the respective inputs, and in parallel with other second inputs of the plurality of second inputs: generating an output according to the function using the input" is shown in '784 page 11, lines 4-36.

As to dependent claim 62, "further comprising, for each output of the plurality of outputs and in parallel with other outputs of the plurality of outputs: combining the output with input data to generate ciphered data" is taught in '784 on page 9, lines 8-31.

As to dependent claim 63, "wherein the combining comprises performing an exclusive-OR operation" is taught in '784 page 9, lines 9-31.

As to independent claim 64, this claim is directed to the apparatus executing the method of claim 55; therefore it is rejected along similar rationale.

As to dependent claims 65-72, these claims contain substantially similar subject matter as claims 56-63; therefore they are rejected along similar rationale.

As to independent claim 73, this claim is directed to an article of manufacture of the method of claim 55; therefore it is rejected along similar rationale.

As to dependent claim 77, the following is not explicitly taught in the combination of '784 and '319: **"wherein the look-up table outputs corresponding to the plurality of inputs comprise a set of outputs, and said method further comprises the step of selecting one of said outputs in response to at least one additional bit included in at least one of said plurality of inputs"** however 3GPP teaches that the two S-boxes, i.e. lookup tables to be implemented in combinational logic to make output in response to bit selection in section 4.5 on page 12.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm taught in '784 and '319 to utilize the KASUMI documentation in order to clarify the invention taught in '784. One of ordinary skill in the art would have been motivated to perform such a modification because as indicated in '784, the invention is directed to an improvement of the convention implementation apply the KASUMI algorithm in the 3GPP system (see '784 page 2, lines 3 et seq.) "However, since the convention implementation technique applying the KASUMI algorithm in the 3GPP system mostly processes the traffic by software, its throughput is lowered, and a large amount of traffic cause the system to have a large amount of load. For example, the RNC switch equipment of the 3GPP system performs the KASUMI encryption algorithm using a power PC processor, and this causes the system to bear a large amount of load, resulting in that the power PC processor should be additionally used to cause a heavy manufacturing cost and inefficiency".

As to dependent claims 78 and 79, these claims contain substantially similar subject matter as claim 77; therefore they are rejected along similar rationale.

10. **Claims 3, 4, 7-10, 14,15, 17-20, 29, 32, 34, 43, and 46,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. World Intellectual Property Organization No. WO 03/050784 (hereinafter '784) International Filing Date 17 April 2002 in view of Luyster U.S. Patent No. 6,751,319 (hereinafter '319) in further view of 3GPP TS 35.202 v3.1.1 Release 1999 (hereinafter 3GPP) in further view of Weybrew et al. U.S. Patent No. 6,931,511 (hereinafter '511).

As to dependent claim 3, the following is not explicitly taught in '784 and '319: **"wherein for each look-up table, the plurality of elements of the look-up table and the plurality of inputs are loaded as vectors and the looking-up comprises, for each of the inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input"** however '511 teaches a plurality of look-up tables being loaded as vectors in col. 8, lines 37-56.

It would have been obvious to one of ordinary skill in the art at the time of the invention an encryption apparatus applying a KASUMI encryption algorithm that utilizes look-up tables taught in the combination of '784 and '319 to include a means to utilize vectors as inputs. One of ordinary skill in the art would have been motivated to perform such a modification in because vector processing allows simultaneous processing of vector data see '511 (col. 4, line 5 et seq.) "Vector processors allow simultaneous processing of a vector of data elements using a single instruction. Table look-up for a vector of data elements maps the data elements of the vector into another vector of data elements using one or an array of tables. In one scenario, each data elements of a vector is looked up from a look-up table, and looking up the data element from the look-up table is independent of looking up other elements from other look-up tables and thus multiple look-ups are preformed sequentially over time".

As to dependent claim 4, "comprising using a vperm (vector permutation) instruction for selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however '511 teaches a vperm instruction in col. 29, lines 44-67.

As to dependent claim 7, "wherein for each time the selection on a remaining number of corresponding outputs is performed, the remaining number of corresponding outputs comprises at least one set of two remaining corresponding outputs and the selection of half of the remaining number of outputs comprises, for each set of two corresponding outputs of the at least one set of two remaining corresponding outputs:" is shown in '784 page 2, lines 25-36;

"replicating the respective bit into a plurality of replicated bits; and using a vector instruction, selecting one of the two remaining corresponding outputs depending on the plurality of replicated bits" however '511 teaches utilizing vectors to select outputs in col. 8, lines 56-65.

As to dependent claim 8, "wherein the vector instruction is a vsel (vector select instruction)" however '511 shows a method to lookup data items indexed by a plurality of vectors in col. 8, lines 56-65.

As to dependent claim 9, "wherein for each input, the first set of bits that define the input comprises five bits, the second set of bits that define the input comprises two bits and

the look-up tables comprise four look-up tables, wherein for each of the four look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and the looking-up comprises for each of the inputs selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however '511 teaches vectors are loaded in a plurality of lookup tables in col 8, lines 37-67.

As to dependent claim 10, "wherein for each input, the first set of bits that define the input comprises four bits, the second set of bits that define the input comprises three bits and the look-up tables comprise eight look-up tables, and wherein for each of the eight look-up tables the plurality of inputs and the plurality of elements of the look-up table are loaded as vectors and for each of the inputs the looking-up comprises selecting one of the plurality of elements of the look-up table using the first set of bits that define the input" however '511 teaches that the vector are indices in col. 8, lines 37-56.

As to dependent claims 14, 15, 17-20, these claim contain substantially similar subject matter as claims 3, 4, 7-10; therefore they are rejected along similar rationale. Note an Altivec processor is shown in '511 col. 5, lines 36-46.

As to dependent claim 29, "wherein for each input of the plurality of inputs, for each look-up table the respective subset of bits of the first plurality of bits that define the input comprises one of 4 and 5 bits and the look-up table is looked-up using a vperm (vector permutation) instruction" however '511 teaches a vperm instruction in col. 29, lines 44-67.

As to dependent claim 32, "wherein the bit shifting instruction comprises one of a vector shift right byte instruction and a vector shift left byte instruction and the bit rotation instruction comprises one of a vector rotate left byte instruction and a vector rotate right byte instruction" however '511 teaches in col. 80, lines 17-41 a macro to rotate vector.

Conclusion

11. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2134
3 April 2008